Soliton

InfoTrace® PLUS Analyzer

PC操作ログ分析による、ITセキュリティソリューション

インフォトレース プラス アナライザー

PC操作ログをエンタープライズ・ビッグデータとして活用し ITセキュリティ・インテリジェンスを実現！

- PC操作ログ分析の課題を一挙解決
- 高速かつ高度なログ検索・分析で、運用負荷を軽減
- Zeronaによる攻撃検出状況の可視化や、影響範囲の素早い把握
- 大規模環境にも対応、スケールアップできる柔軟な構成

内部不正、情報漏えい、サイバー攻撃対策の答えは

エンタープライズ・ビッグデータの活用によるITセキュリティ

高度化するサイバー攻撃や内部不正による情報漏えいのリスクが高まり、より強固なセキュリティ対策が求められる中、エンタープライズ・ビッグデータともいえる、PC操作ログの活用が見直されています。
InfoTrace PLUS Analyzerは、これまで有効活用が難しいとされてきたPC操作ログから、すばやくインシデントを洗い出し、ITセキュリティに悩む管理者を助ける、次世代のPC操作ログソリューションです。

内部不正動機が低下する対策

- 社内システム操作の証拠が残る 54%
- 顧客情報などの重要な情報にアクセスした人が監視される（アクセスログ監視） 38%
- これまでに同僚が行ったルール違反が発覚し処罰されたことがある 36%
- 社内システムにログインするためのIDやパスワードの管理を徹底する 32%
- 顧客情報などの重要な情報を持ちだした場合の罰則規定を強化する 31%

IPA「組織内部者の不正行為によるインシデント調査」報告書、2012.7

ログ分析の課題

- 不正を見つけるのが難しい 86%
- 複数製品のログの相関分析が難しい 78%
- ログ分析のスキル不足 55%
- データの正規化が難しい 45%
- 統合ログ分析ツールにログを送付する前のデータ削減が難しい 43%

SANS Log and Event Management Survey Results, 2012.5

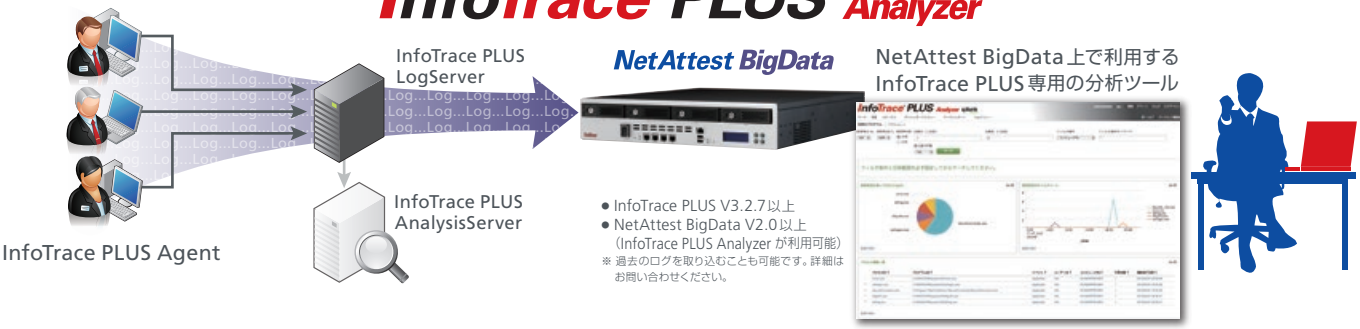
InfoTrace® PLUS

操作ログ記録の事実を利用者に周知する「抑止効果」だけではなく、インシデント発生時に証跡として利用可能な強固な操作ログ取得・保全機能を持つ情報漏洩対策・IT統制ソリューションとして、多くの組織・企業で採用されています。

NetAttest BigData

導入や運用が簡単なログ分析アプライアンスです。ソリトン製品のログ分析を標準搭載し、専門知識が無くてもすぐに高度な分析結果を得ることができます。

InfoTrace® PLUS Analyzer



- InfoTrace PLUS V3.2.7以上
- NetAttest BigData V2.0以上（InfoTrace PLUS Analyzer が利用可能）

※ 過去のログを取り込むことも可能です。詳細はお問い合わせください。

圧倒的なパフォーマンス

1万台を超える大規模環境対応を可能にする圧倒的なパフォーマンスにより高度な分析結果をご提供します。

ログの格納性能	検索レスポンス
約12万/秒	約30億レコード※のログ検索結果を約1分で表示

※ PC2万台からのログ約1ヶ月分を想定、当社調べ。パフォーマンスは環境等にも依存します。詳しくはお問い合わせください。

エンタープライズ・ビックデータの活用にある

ログの有効活用に欠かせない様々な機能が満載！

直観的に全体の状況把握ができるほか、隠れたセキュリティインシデントを徹底的に洗い出すこともできます。

PC操作状況の概要

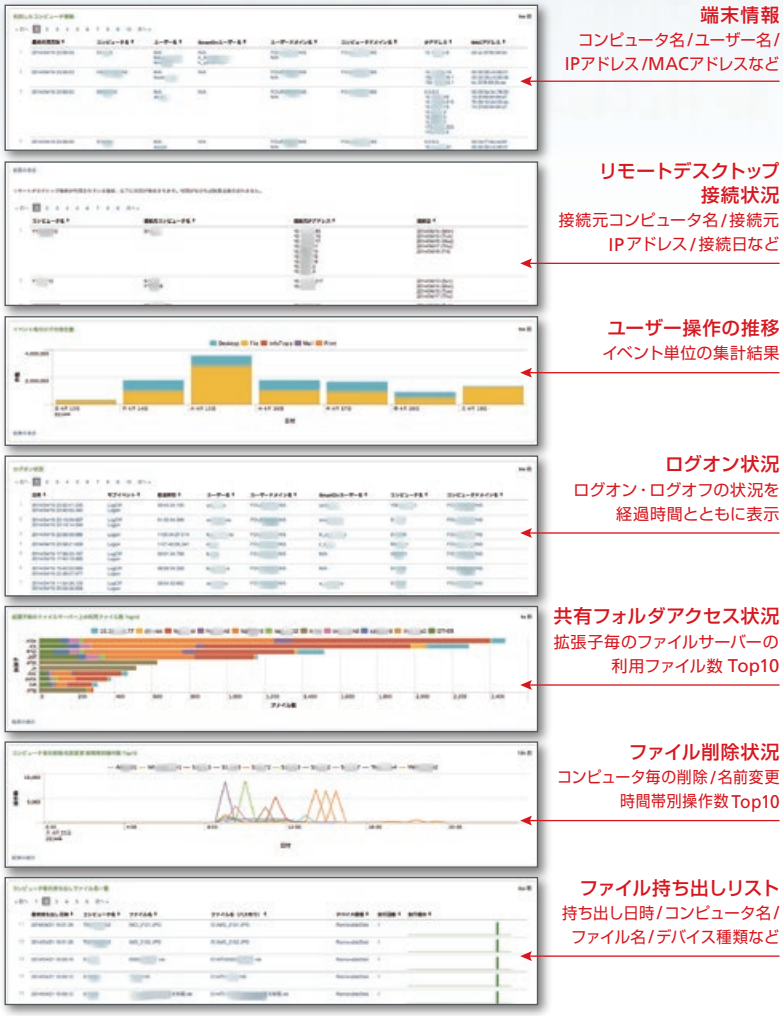
先週と今週の傾向比較で簡単把握

集計機能で利用量も簡単把握

印刷、アプリケーション操作の回数と量を簡単に集計

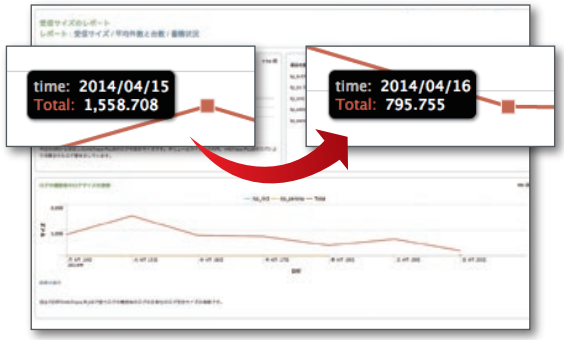
目的別の各種監査レポート

日次、週次、月次の分析からクリックによるドリルダウンだけで徹底的にチェック



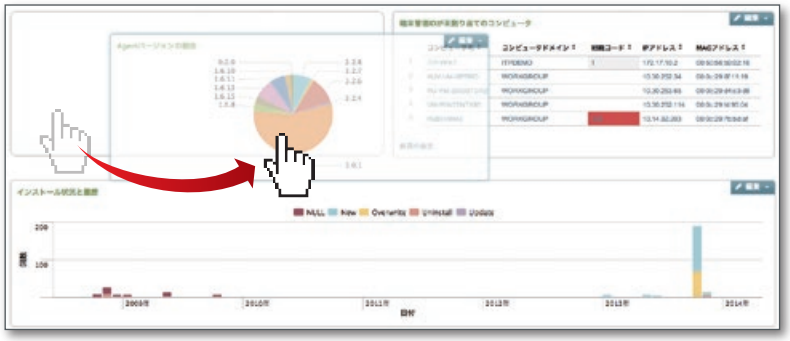
ログ取得設定のチューニング

ログ取得の無駄を省き効率良い運用を実現する分析が可能



柔軟なレポートカスタマイズ

ビュー画面のカスタマイズに対応し、パネルの追加やマウス操作での並べ替えも可能



InfoTrace® PLUS Analyzer

InfoTrace PLUSで記録可能なPC操作（概要）

単なる抑止効果だけではなく、インシデント発生時にも役立つログをしっかりと記録する、国内実績No.1※のPC操作ログソフトウェア

- ローカルファイルの参照・削除・名前変更・コピー
- プリントスクリーンの実行
- PC電源オン・オフ、セーフモード起動 Windowsログオン・ログオフ
- プリンタでの印刷 印刷機能でのファイル出力
- ネットワーク上のファイルの参照・削除・名前変更・コピー
- クリップボードを利用した文字列コピー
- PCの操作中断・再開 スクリーンセイバーの起動・終了
- アプリケーションごとの起動回数・起動時間、ウィンドウタイトル
- コマンドプロンプトからのファイル操作
- 外部ストレージファイルの参照・削除・名前変更・コピー
- Internet Explorerでアクセスしたurl
- リモートデスクトップでのPC操作・接続元IP
- アプリケーションからのファイル操作
- 送信メールの宛先・件名 添付ファイル名、メーラー (Notesメールにも対応)

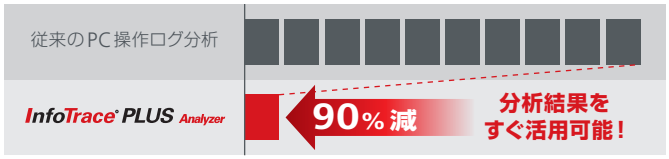
※ ネットワーク・セキュリティビジネス調査総覧, 富士キメラ総研 2013

ログ分析コストの削減

目的に合わせて整理された複数の情報を一つのレポートで表現することにより、インシデント調査や行動監査のための作業量を削減します。必要な情報と関連情報を、一度で確認できます。

■ 従来型PC操作ログ分析の状況

- 煩雑な分析集計作業の定期実施
  - ・イベントで絞込み、結果をファイル出力した上で、Excelやスクリプトで集計
  - ・イベント、コンピュータ、ユーザー単位で、再集計
  - ・グラフィカルに整形してレポート作成

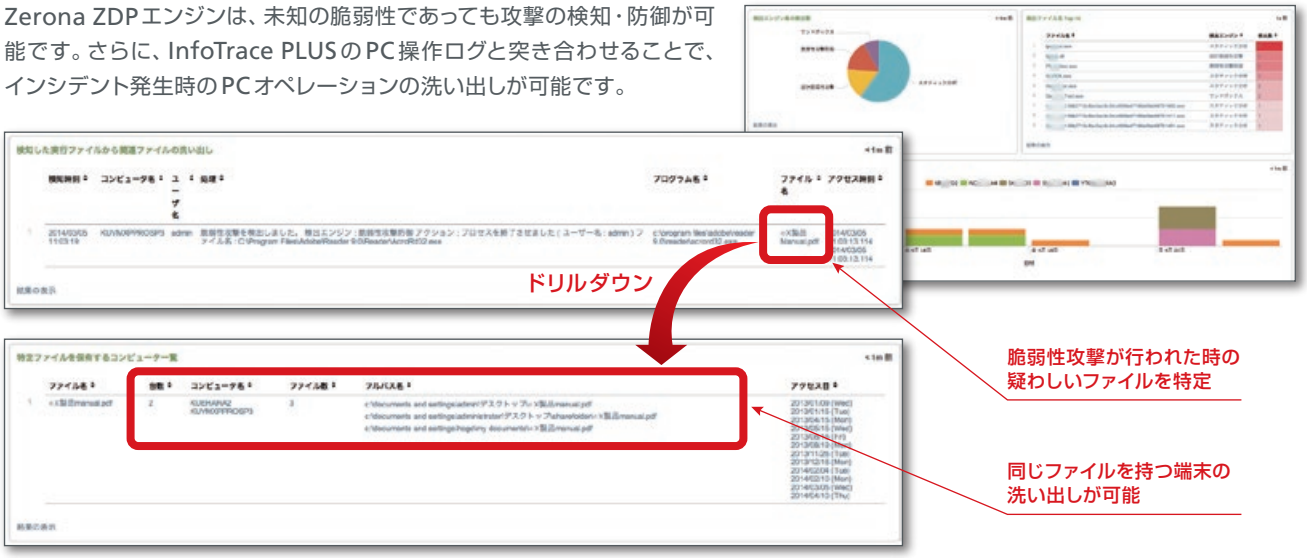


■ InfoTrace PLUS Analyzerなら

- 最低限の条件（コンピュータ名など）を指定するだけで目的の情報をグラフィカルに可視化
- 効果を確認しながら、ログチューニングが可能

Zerona との併用で、標的型サイバー攻撃対策を強化

Zerona ZDPエンジンは、未知の脆弱性であっても攻撃の検知・防御が可能です。さらに、InfoTrace PLUSのPC操作ログと突き合わせることで、インシデント発生時のPCオペレーションの洗い出しが可能です。



※ 記載の製品名は、各社の商標または登録商標です。

⚠ 安全に関するご注意	正しく安全にお使いいただくために、ご使用の前に必ず「取扱説明書」をお読みください。

Soliton

株式会社ソリトンシステムズ　http://www.soliton.co.jp/

〒160-0022　東京都新宿区新宿 2-4-3

TEL 03-5360-3811　FAX 03-3356-6354　netsales@soliton.co.jp

大阪営業所 06-6821-6777　福岡営業所 092-263-0400

名古屋営業所 052-963-9700　東北営業所 022-716-0766

札幌営業所 011-242-6111

このカタログは 2014年4月現在のものです。仕様、デザインは予告なく変更することがあります。　ITPA-1404A